DOI 10.31891/2307-5732-2023-327-5-237-242
УДК 004.6:336.7

ПАШОРІН ВАЛЕРІЙ
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0001-6165-1147
e-mail: v.pashorin@e-u.edu.ua
ЯРОВИЙ РОМАН
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0001-8978-8137
e-mail: roman.yaroviy@e-u.edu.ua
ЗАХАРЕНКОВ ДМИТРО
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0003-3951-022X
e-mail: dmit.zakharen@gmail.com
МИЛАШЕНКО ВІКТОР
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0002-1434-7609
e-mail: viktor.mylashenko@e-u.edu.ua

ЗАХИСТ КРИПТОВАЛЮТ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У статті досліджені питання реалізації механізмів забезпечення безпеки генерації, зберігання та передачі криптовалюти. Показані основні напрями рішення проблеми захисту цифрової валюти від можливих шахрайських дій під час транзакцій і зберіганні її в електронних гаманцях. Розкрито сутність механізмів забезпечення безпеки криптовалюти Біткойн. Визначені основні проблеми захисту криптовалют, які пов'язані з хакерськими атаками та шахрайством, безпекою електронних гаманців та вразливостями смарт-контрактів. Зазначено, що незважаючи на використання передових криптографічних методів, криптовалюти залишаються мішенню для хакерів. Наведено фундаментальні розбіжності між криптовалютою та цифровою валютою. Визначено властивості криптографічних хеш-функцій, які застосовуються для захисту транзакцій від можливих фальсифікацій чи підмін блоків транзакцій електронного реєстру. Наданий скорочений алгоритм генерації адреси електронного гаманця. Надані рекомендації щодо вдосконалення механізмів захисту від нових типів атак, розвиток більш ефективних алгоритмів хешування та підвищення зручності користування електронними гаманцями. Також відзначено важливість розробки та впровадження стандартів безпеки для криптовалют, що сприятиме їх широкому використанню та інтеграції в фінансові системи.

Ключові слова: цифрова валюта, криптосистема, блокчейн, біткойн, хеш-функція, електронний гаманець.

PASHORIN VALERIY, YAROVOY ROMAN, ZAKHARENKOV DMYTRO, MYLASHENKO VIKTOR
Private higher education institution "European University"

PROTECTION OF CRYPTOCURRENCIES: CURRENT CHALLENGES AND PROSPECTS FOR DEVELOPMENT

The article investigates the issues of implementing mechanisms for ensuring the security of cryptocurrency generation, storage and transmission. The author shows the main directions of solving the problem of protecting digital currency from possible fraudulent actions during transactions and its storage in electronic wallets. The essence of the mechanisms for ensuring the security of the Bitcoin cryptocurrency is revealed. The main problems of cryptocurrency protection related to hacker attacks and fraud, security of electronic wallets and vulnerabilities of smart contracts are identified. It is noted that despite the use of advanced cryptographic methods, cryptocurrencies remain a target for hackers. The ECDSA algorithm with proven cryptographic strength is used to generate electronic wallet keys. The use of the peer-to-peer architecture of a network of distributed ledger nodes and blockchain technology in the cryptocurrency payment system significantly increases the level of security of cryptocurrency use. The fundamental differences between cryptocurrencies and digital currencies are presented. The properties of cryptographic hash functions used to protect transactions from possible falsification or substitution of transaction blocks of the electronic registry are determined. A shortened algorithm for generating an electronic wallet address is presented. Recommendations are made to improve protection mechanisms against new types of attacks, develop more efficient hashing algorithms, and improve the usability of electronic wallets. The author also emphasizes the importance of developing and implementing security standards for cryptocurrencies, which will facilitate their widespread use and integration into financial systems.

Keywords: digital currency, cryptosystem, blockchain, bitcoin, hash function, electronic wallet.

Постановка проблеми

Динаміка впровадження інформаційних технологій в банківській сфері в останні десятиліття не може не вражати. Складно переоцінити перехід на електронні платіжні системи, використання електронного цифрового підпису в документообігу банків, застосування електронних грошей або цифровий валюти. Однак вкрай важливо концентруватися не тільки на позитивних моментах нових технологій, але і на питаннях безпеки їх застосування, особливо коли мова йде про гроші. Досить актуальним є вивчення питання безпеки криптовалюти. Зокрема, проблеми, що виникають через вразливості смарт-контрактів, загрози з боку хакерів,

а також незахищеність електронних гаманців, можуть мати значні негативні наслідки для користувачів криптовалют.

Основними проблемами захисту криптовалют є хакерські атаки та шахрайство, безпека електронних гаманців та вразливості смарт-контрактів. Незважаючи на використання передових криптографічних методів, криптовалюти залишаються мішенню для хакерів. Злами бірж, викрадення коштів та шахрайські ICO є реальними загрозами, які можуть призвести до значних фінансових втрат. Смарт-контракти, які є основою багатьох криптовалютних платформ, часто мають програмні помилки, що можуть бути використані зловмисниками. Невдала реалізація смарт-контракту може призвести до втрати коштів користувачів. Електронні гаманці, які зберігають приватні ключі користувачів, є основною мішенню для хакерів. Компрометація цих гаманців може призвести до викрадення криптовалют.

Захист криптовалют є багатогранною проблемою, що потребує комплексного підходу. Необхідно постійно вдосконалювати механізми безпеки, проводити аудит смарт-контрактів, підвищувати безпеку електронних гаманців та розробляти ефективні регуляторні заходи. Тільки таким чином можна забезпечити стійкий розвиток криптовалют та їх інтеграцію у глобальну фінансову систему.

Аналіз останніх досліджень і публікацій

З моменту своєї появи в 2009 році криптовалюта зацікавила безліч дослідників з різних сфер людської діяльності. Спроби зрозуміти, що таке цифрова валюта на блокчейні і як вона працює, робилися в провідних світових університетах і дослідницьких центрах. Так, в 2017 році кілька наукових робіт, присвячених криптовалюті, вийшло в Кембриджському університеті [1]. Сотні експертів з усього світу намагаються передбачити, куди піде курс цифрових грошей, не особливо заглиблюючись в фундаментальний аналіз причин їхнього успіху. Є й інші дослідження - їх автори не претендували на глибоке розгляд феномена криптовалюти, а концентрувалися на приватних питаннях [2-4]. Одним із таких питань, яке, на наш погляд, пов'язане також із неочікуваним успіхом використання криптовалюти, є питання безпеки криптовалюти.

Метою статті є дослідження застосовуваних технологій безпеки використання цифрової валюти на прикладі криптовалюти Біткойн та безпекових механізмів децентралізованої розподіленої мережі блокчейн, на якій базується криптовалюта Біткойн.

Матеріали та методи

Інформаційною базою дослідження стали праці закордонних вчених, звіти фінансових установ [5], електронні ресурси, що піднімають проблеми використання цифрової валюти. Для досягнення поставленої мети використано наукові методи теоретичного узагальнення, аналізу, синтезу та аналогій.

Результати дослідження

Цифрова валюта - це електронний аналог звичайної валюти, яка існує в віртуальному форматі, без фізичного еквіваленту в реальному світі, але має всі характеристики валюти. Як і класичні гроші, цифрову валюту можна получати, переводити або обмінювати на іншу валюту, оплачувати нею товари та послуги. Цифрова валюта не має державних кордонів: гроші з електронного гаманця, що відповідає цій валюті, можуть бути переведені відкіля завгодно і куди завгодно.

Криптовалюта є різновидом цифрової валюти. Це актив, який використовується в якості засобу обміну і вважається надійним тому що в його основі лежить криптографія, технологія блокчейн і розподілений реєстр. Не дивлячись на те, що криптовалюта - це різновид цифрової валюти, між криптовалютою та цифровою валютою можна виділити фундаментальні розбіжності.

1. *Цифрова валюта централізована.* Платіжна система цифрової валюти передбачає наявність центрального органу, який контролює мережеві транзакції. Цей орган може скасувати або заморозити транзакцію на вимогу, чи в разі підозри шахрайства або незаконної операції.

Платіжна система криптовалюти має пірінгову архітектуру (P2P), тобто вся система, що забезпечує здійснення транзакцій і збереження інформацію про них, заснована на децентралізованій комп'ютерній мережі. Не існує центрального сервера, який вів би облік всіх транзакцій криптовалюти. Вся інформація про транзакції зберігається на тисячах серверів, причому на кожному з них зберігається повна копія реєстру, що включає всі транзакції криптовалюти, здійснені будь-коли і будь-де. Таким чином, безліч комп'ютерів по всьому світу утворюють гігантську автоматичну, працюючу цілодобово, електронну платіжну систему.

Децентралізація підвищує рівень безпеки криптовалюти, оскільки якщо ще і можна допустити можливість зловмисного втручання в роботу якогось одного центрального органу управління, то будь-які спроби внесення змін на окремі вузли розподіленої системи просто безглузді: доведеться зламати тисячі комп'ютерів одночасно, а не один центральний сервер. Додавання або видалення транзакцій в розподіленої системі повинні бути прийняті всіма вузлами розподіленої мережі, в іншому випадку вони відкидаються. Таким чином, децентралізація і застосування розподіленого реєстру в обліку криптовалюти, є важливим аспектом безпеки самої криптовалюти.

2. *Цифрова валюта не підтримує анонімність*. Для користування цифровою валютою потрібна ідентифікація користувача в платіжній системі та реєстрація певних документів, виданих банками або державними структурами. При цьому встановлюється особа, що здійснює операцію з валютою.

Для покупки, продажу, інвестування і будь-яких інших маніпуляцій з криптовалютою ніякої реєстрації особистості не потрібно, не потрібно також вказувати будь-якого роду особисті дані відправника та отримувача коштів. Для здійснення транзакції необхідно знати тільки публічний ідентифікатор одержувача (номер гаманця для криптовалюти), який, до речі, може змінюватися для кожної транзакції.

Для запобігання шахрайству при транзакціях використовується електронний цифровий підпис (ЕЦП) власника криптовалюти. Підписуючи передачу прав з використанням ЕЦП, власник накладає на себе зобов'язання передачі. Алгоритми ЕЦП, що застосовуються при передачі криптовалюти не відрізняються від алгоритмів ЕЦП, застосовуваних в банківській та інших економічних сферах. Різниця в застосуванні ЕЦП тут полягає в тому, що при перевірці ЕЦП транзакцій в банківській сфері встановлюється крім іншого і особистість власника ЕЦП. При перевірці ЕЦП транзакцій криптовалюти визначається тільки номер електронного гаманця власника криптовалюти, сам же власник залишається невідомим. З точки зору захисту персональних даних анонімність також може розглядатися як елемент технології безпеки.

3. *Цифрова валюта непрозора*. Інформація про транзакції цифрової валюти конфіденційна і відповідно недоступна для публічного перегляду.

Транзакції криптовалюти навпаки прозорі. Можна побачити список транзакцій любого власника криптовалюти знаючи його публічний (відкритий) ключ ЕЦП, оскільки всі його дії з криптовалютою фіксуються в блокчейні.

Більш того, для криптовалюти виключено шахрайство пов'язане з транзакцією неіснуючих активів, оскільки при будь-якій транзакції передаються і відповідно перевіряються платіжною системою криптовалюти всі надходження в і витрати з електронного гаманця, з якого здійснюється транзакція. Власник електронного гаманця не може передати з нього суму більшу, ніж він отримав на нього з підтверджених системою транзакцій. Безумовно така технологія також є перш за все технологією, що забезпечує безпеку використання криптовалюти.

Як вже зазначалось вище, надійність та безпека функціонування платіжної системи криптовалюти заснована на використанні криптографічних методів. Можливо в силу домінуючої ролі криптографії в платіжній системі криптовалюти і з'явилася приставка крипто в назві цього виду цифрової валюти. Слід зазначити що кріпторафія, як механізм забезпечення безпеки в платіжній системі криптовалюти, використовується, по-перше, на етапах зберігання та передачі криптовалюти, а, по-друге, застосовується при формуванні розподіленого реєстру транзакцій, які зберігаються в блоках. У першому випадку використовується так звана сучасна криптографія з відкритим ключем для реалізації технології ЕЦП та класична або симетрична криптографія для можливого захисту сховища електронних гаманців і трафіку транзакцій.

У другому випадку при формуванні блоків транзакцій застосовуються криптографічні хеш-функції для захисту транзакцій від можливих фальсифікацій чи підмін блоків транзакцій електронного реєстру. Тут важливо, що з усього класу можливих хеш - функцій застосовуються саме криптографічні хеш-функції, що володіють такими властивостями, які гарантують безпеку результатів своєї роботи від підміни або змін, а саме такими властивостями як:

- детермінованість, тобто результат роботи хеш-функції завжди одне і теж хеш-значення, якщо вхідні дані для цієї функції незмінні;
- односпрямованість - властивість функції при якій швидко і легко обчислюється значення самої функції за відомим значенням аргументу, а зворотна процедура - обчислення аргументу за відомим значенням функції є вкрай трудомістким завданням;
- колізійна стійкість - незначна ймовірність генерації однакового хеш-значення при різних вхідних параметрах;
- розсіюваність. Ця властивість полягає в тому, що при найменшій зміні тексту, результат хешування змінюється кардинально. Наприклад, якщо текст для хешування має вигляд: «Європейський університет», то хешування за допомогою алгоритму SHA-256 дасть наступний результат:

0dbc514017f041bf8c0a77ce045dfa2347b98b7525bba7da3f105cf9458d8f24

Додавши у вхідний текст всього один пробіл між двома словами отримаємо зовсім інший результат хешування:

8b39bc30965d990412a3d27128279e00dc5ef2a08fb3e89a74bd358736ec69cd

Криптографічні методи застосовуються, крім перерахованого вище, і при самій генерації одиниць криптовалюти, а саме при обробці чергового блоку транзакцій здійснюється пошук хеш-значення поточного блоку з заданим рівнем складності. У визначенні криптовалюти, наведеному в Оксфордському словнику, відзначається цей факт: «... a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank [6].

Найбільш відома криптовалюта - це Біткойн. Біткойном називається також і електронна платіжна система, через яку здійснюються операції з цією валютою.

Платіжна система криптовалюти Біткойн децентралізована і функціонує на вузлах розподіленої мережі, що підтримують цю систему. У біткойн - системі для зберігання виконаних транзакцій використовується ланцюжок блоків (блокчейн). Кожен блок такого ланцюжка містить заголовок і обмежений список транзакцій. У заголовку записані параметри, серед яких є хеш-значення попереднього блоку. Сам попередній блок має точно таку ж структуру: заголовок з хеш-значенням відповідно попереднього блоку і список попередніх транзакцій і т д. Таким чином весь ланцюжок блоків зберігає всі транзакції за весь час роботи біткойн-системи. Безпеку такого зберігання можна проаналізувати, якщо детальніше розглянути роботу платіжної системи.

Система працює за такими правилами:

1. Клієнт, здійснюючи транзакцію, передає інформацію про неї в мережу платіжної системи, яка розсилає її всім вузлам мережі.
2. Кожен вузол мережі об'єднує транзакції, що прийшли за певний період в блок і обчислює хеш-значення всього блоку, яке повинно задовольняти заданому рівню складності.
3. Як тільки хеш-значення з заданим рівнем складності для всього блоку транзакцій буде обчислено, вузол мережі, який виконав це, відправляє тепер уже новий блок транзакцій в розподілену мережу.
4. Вузли мережі перевіряють блок і транзакції усередині нього на валідність і приймають цей блок тільки якщо всі транзакції в ньому коректні і не використовують уже витрачені кошти.
5. Свою згоду з новими даними вузли висловлюють починаючи роботу над наступним блоком, використовуючи хеш-значення попереднього блоку.

При такій схемі роботи платіжної системи, щоб ввести зміни в якусь транзакцію в блоці без втрати довіри до нього з боку всієї мережі, потрібно буде забезпечити незмінність хеш-значення всього блоку. А це практично неможливо, так як використовується криптографічно стійка хеш-функція для отримання хеш-значення всього блоку. Щоб платіжна система прийняла блок транзакцій вже зі зміненим хеш - значенням всього блоку, потрібно буде змінити хеш-значення і в подальшому блоці, в заголовку якого міститься інформація про хеш-значення попереднього блоку і т. д. Таким чином, для того, щоб поміняти інформацію про транзакції в одному з блоків, потрібно буде генерувати весь ланцюжок блоків. Імовірність реалізації такої процедури незначна і сильно корелює з обчислювальною потужністю мережі біткойн, яка на сьогоднішній день перевищує обчислювальні ресурси гіпотетичної мережі з 500 найпотужніших суперкомп'ютерів, наявних в світі.

За даними bitcoinwatch.com, хешрейт мережі біткойн перевищив 1 екзафлоп. Звичайно, це приблизне число, оскільки сам процес обчислення хеш-значень окремих транзакцій і їх блоків в мережі не вимагає проведення операцій з плаваючою комою.

Щоб надійно функціонувати, система блокчейн повинна весь час створювати нові блоки, причому в розподіленій системі нові блоки повинні створюватися не єдиним суб'єктом, а мережею в цілому. Консенсус у всій мережі по включенню конкретного блоку в ланцюг (після його верифікації) при відсутності довірчих відносин між вузлами мережі досягається угодою, що в ланцюжок розподіленого реєстру буде внесений саме той блок транзакцій з великого числа претендентів, який задовольняє вимогам до хеш-значення цього блоку. Хеш-значення блоку транзакцій в свою чергу є результатом роботи криптографічного алгоритму хешування. Багаторазове застосування цього алгоритму, з циклічною зміною заданої константи на вході, вимагає значних обчислювальних ресурсів, рівень яких залежить від заданих вимог до хеш-значення блоку. Перевірка ж хеш-значення на відповідність заданим вимогам не має обчислювальної складності, тому криптографічне хешування є гарною реалізацією відомого механізму досягнення консенсусу «proof-of-work» (доказ роботи) в розподіленій децентралізованій платіжній системі [7].

Само по собі хешування не несе ніякої корисної мети крім збільшення складності пошуку правильного блоку. Це гарантує, що ніхто в поодинці, з будь-яким існуючим набором ресурсів, не зможе взяти під контроль всю систему. Безумовно, такий підхід також є технологією безпеки.

Важливим елементом платіжної системи криптовалюти Біткойн є електронні гаманці, які можна розглядати як аналог банківських рахунків в централізованій платіжній системі. На даний момент вже існує досить багато різних реалізацій електронних гаманців (програмних, апаратних, гібридних, онлайн-гаманців), але в більшості випадків спрямування цих інструментів приблизно однаково:
- генерація і зберігання ключів (приватного і публічного) для постановки та перевірки ЕЦП;
- здійснення транзакцій;
- генерація біткойн-адрес для вхідних транзакцій;
- доступ до історії транзакцій та інформації про поточний баланс.

Безпека самого електронного гаманця багато в чому заснована на безпеці операцій з ключами.

Для публічного ключа не існують якісь вимоги щодо забезпечення його таємності. Більш того він відомий в платіжній системі, так як публічний ключ, а точніше хеш-значення від публічного ключа є адресою електронного гаманця куди переводиться криптовалюта Біткойн. Адреса електронного гаманця є унікальна послідовність символів, що генерується платіжною системою. Процедура генерації є досить складною сукупністю криптографічних перетворень з метою підвищення безпеки використання електронного гаманця. Нижче наданий скорочений алгоритм генерації адреси електронного гаманця [8].

1. Вибирається відкритий ключ довжиною 65 байт (1 байт - ідентифікатор, а наступні 64 байти відповідають координаті X і координаті Y однієї з точок еліптичної кривої в кінцевому полі):

04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e5
1ec112de5c384df7ba0b8d578a4c702b6bf11d5f

2. Проводиться хешування відкритого ключа по алгоритму SHA-256:

261c1eb21fc4708c6acbe1cfc6d4565652e9e768b620782898936b93000a6c02

3. Виконується хешування попереднього результату роботи за алгоритмом RIPEMD-160 для отримання 20-байтної адреси:

62e907b15cbf27d5425399ebf6f0fb50ebb88f18

4. Додається байт-ідентифікатор перед хеш-значенням і контрольна сума з 4 байт в кінці хеш-значення для перевірки коректності введення адреси.

5. Результат конвертується в заданий в біткойн-мережі формат base58.

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Це і є адреса електронного гаманця. Такий формат запису використовується для компактності, хоча по суті ключ представляє собою дуже велике просте число.

Публічний ключ використовується також платіжною системою для перевірки легальності транзакцій від власника приватного ключа, яким підписується транзакція, оскільки, як відомо, публічний і приватний ключі математично пов'язані між собою.

Приватний ключ також формується платіжною системою. Обчислення приватного ключа за відомим публічним ключем є складною математичною задачею, оскільки використовується алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm). Крипостійкість цього алгоритму ґрунтується на проблемі дискретного логарифма в групі точок еліптичної кривої. Криптосистеми на еліптичних кривих використовуються сьогодні практично у всіх сучасних технологіях захисту цифрової інформації і гарантують високий рівень безпеки цифрових активів. При використанні цього алгоритму приватний ключ практично неможливо підібрати обчислювальним шляхом, але можна вкрасти. Тому необхідно зберігати значення приватного ключа в таємниці, оскільки той, хто знає або має доступ до приватного ключа, відповідно має доступ і до електронного гаманця.

Висновки

Застосування сучасних криптографічних методів для нової цифрової валюти забезпечує необхідний рівень безпеки від можливих прихованих і відкритих шахрайських дій на всіх етапах життєвого циклу криптовалюти: генерації, передачі, зберіганні. Важливо, що для генерації ключів електронного гаманця використовується алгоритм ECDSA з доведеною крипостійкістю. Використання ж в платіжній системі криптовалюти пірінгової архітектури мережі вузлів розподіленого реєстру і технології блокчейн істотно підвищують рівень безпеки застосування криптовалюти. Подальші дослідження можуть бути спрямовані на вдосконалення механізмів захисту від нових типів атак, розвиток більш ефективних алгоритмів хешування та підвищення зручності користування електронними гаманцями. Також важливо розробляти та впроваджувати стандарти безпеки для криптовалют, що сприятиме їх широкому використанню та інтеграції в фінансові системи.

Література

1. Dr Garrick Hileman. Michel Rauchs. Global cryptocurrency benchmarking study. Cambridge Centre for Alternatve Finance. 2017.
2. Juan A. Garay. Aggelos Kiayias. Nikos Leonardos.The Bitcoin Backbone Protocol: Analysis and Applications. 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II. p.281-310.
3. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. URL: http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf
4. Reuben Grinberg. Bitcoin: An Innovative Alternative Digital Currency. Hastings Science and Technology Law Journal. January 6, 2012. URL: http://scienceandtechlaw.org/bitcoin-an-innovative-alternative-digital-currency/
5. CPMI report on digital currencies. Digital currencies. Committee on Payments and Market Infrastructures. November 2015.
6. Cryptocurrency. URL: https://en.oxforddictionaries.com/definition/cryptocurrency
7. Nakamoto S. Bitcoin: F Peer-to-Pear Electronic Cash System. URL: http://bitcoin.org/bitcoin.pdf
8. Technical background of Bitcoin addresses. URL: http://en.bitcoin.it
9. Тимошенко О. І., Литвиненко Л. О., Колодінська Я. О. Загрози та безпека кіберпростору в умовах сучасних викликів: проблеми, інструменти, рішення. Актуальні питання забезпечення кібербезпеки та захисту інформації: колективна монографія / за заг. наук. ред. А.М. Давиденко, Київ: Європейський університет, 2023. – С. 10-18.
10. Троян К.М., Скляренко О.В. Практичні кейси та перспективи розвитку технологій штучного інтелекту //Цифрова трансформація в економіці, менеджменті і бізнесі. Проблеми науки, практики та освіти: Зб. матеріалів XXVIII Міжн. наук.- практ. конф., Київ, 24.11.2022 р.; К.: Вид-во Європейського університету, 2023 – С. 66-68.

References

1. *Dr Garrick Hileman*. Michel Rauchs. Global cryptocurrency benchmarking study. Cambridge Centre for Alternatve Finance. 2017.
2. *Juan A. Garay*. Aggelos Kiayias. Nikos Leonardos.The Bitcoin Backbone Protocol: Analysis and Applications. 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II. p.281-310.
3. *Joseph Bonneau*, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. URL: http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf
4. *Reuben Grinberg*. Bitcoin: An Innovative Alternative Digital Currency. Hastings Science and Technology Law Journal. January 6, 2012. URL: http://scienceandtechlaw.org/bitcoin-an-innovative-alternative-digital-currency/
5. *CPMI report* on digital currencies. Digital currencies. Committee on Payments and Market Infrastructures. November 2015.

6. Cryptocurrency. URL: https://en.oxforddictionaries.com/definition/cryptocurrency
7. *Nakamoto S.* Bitcoin: F Peer-to-Pear Electronic Cash System. URL: http://bitcoin.org/bitcoin.pdf
8. Technical background of Bitcoin addresses. URL: http://en.bitcoin.it
9. Tymoshenko O. I., Lytvynenko L. O., Kolodinska Y. O. Threats and security of cyberspace in the context of modern challenges: problems, tools, solutions. Topical issues of cybersecurity and information protection: a collective monograph / edited by A. Davydenko, Kyiv: European University, 2023. pp. 10-18.
10. Troyan K.M., Skliarenko O.V. Practical cases and prospects for the development of artificial intelligence technologies // Digital transformation in the economy, management and business. Problems of science, practice and education: Proceedings of the XXVIII International Scientific and Practical Conference, Kyiv, 24.11.2022; K.: European University Press, 2023 - P. 66-68.